Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-6 (Cancelled)

7. (Currently Amended) A method for operating a communication terminal for packet-oriented data transmission, the method comprising:

~~storing status information for a communication terminal in a memory unit associated with the communication terminal;~~

depositing a public key of a first control unit such that at least one second control unit is able to access the public key;

providing ~~the~~ status information to a communication terminal, the status information comprising ~~with~~ a digital signature calculated from ~~the~~ status information of the communication terminal by a private key of the first control unit, ~~for an asymmetrical encoding method, wherein the private key is associated with a~~ the first control unit being associated with the communication terminal for the resolution and/or conversion of network addresses; ~~addresses and is stored remote from the communication terminal;~~

storing the status information in a memory unit associated with the communication terminal;

transmitting a request to associate the communication terminal with at least one second control unit if the first control unit fails, the request comprising the status information and the digital signature;

checking the digital signature with the at least one second control unit, the at least one second control unit configured to access the public key of the first control unit to check the digital signature; ~~signature;~~ and

associating the communication terminal with the at least one second control unit if ~~in~~ the ~~event of~~ checking of the digital signal results in a positive check result.

8. (Currently Amended) The method according to claim 7, wherein the status information of the communication terminal is updated at least at a predefinable time upon ~~the~~ initiation of the first or at least one second control unit.

9. (Currently Amended) The method according to claim 7, wherein the digital signature is calculated from a hash value ascertained ~~acquired~~ for the status information of the communication terminal. ~~information.~~

10. (Currently Amended) The method according to claim 8, wherein the digital signature is calculated from a hash value ascertained ~~acquired~~ for the status information of the communication terminal. ~~information.~~

11. (Currently Amended) The method according to claim 7, wherein a hash value is calculated for the status information of the communication terminal by the at least one second control unit for ~~the purposes of~~ checking the digital signature and said hash value is compared

for a match with a digital signature decoded by using ~~a~~ the public key ~~associated with~~ of the first control unit.

12. (Currently Amended) The method according to claim 8, wherein a hash value is calculated for the status information of the communication terminal by the at least one second control unit for ~~the purposes of~~ checking the digital signature and said hash value is compared for a match with a digital signature decoded by using ~~a~~ the public key ~~associated with~~ of the first control unit.

13. (Currently Amended) The method according to claim 9, wherein the hash value is calculated for the status information of the communication terminal for ~~the purposes of~~ checking the digital signature, and wherein the hash value is compared for a match with a digital signature decoded by using ~~a~~ the public key ~~associated with~~ of the first control unit.

14. (Currently Amended) The method according to claim 10, wherein the hash value is calculated for the status information of the communication terminal for ~~the purposes of~~ checking the digital signature, and wherein the hash value is compared for a match with a digital signature decoded by using ~~a~~ the public key ~~associated with~~ of the first control unit.

15. (Currently Amended) The method according to claim 9, wherein a message digest no. 5 algorithm is used ~~for calculating~~ to calculate the digital signature.

16. (Currently Amended) The method according to claim 10, wherein a message digest no. 5 algorithm is used ~~for calculating~~ to calculate the digital signature.

17. (Currently Amended) The method according to claim 11, wherein a message digest no. 5 algorithm is used ~~for calculating~~ to calculate the digital signature.

18. (Currently Amended) The method according to claim 12, wherein a message digest no. 5 algorithm is used ~~for calculating~~ to calculate the digital signature.

19. (Currently Amended) The method according to claim 13, wherein a message digest no. 5 algorithm is used ~~for calculating~~ to calculate the digital signature.

20. (Currently Amended) The method according to claim 14, wherein the message digest no. 5 algorithm is used ~~for calculating~~ to calculate the digital signature.

21-25 (cancelled)

26. (Currently Amended) ~~Computer~~ A communication terminal comprising at least one processor operatively connected to at least one memory within a housing and a readable medium stored in the at least one memory, the readable medium comprised of ~~comprising~~ executable code readable by the at least one ~~a computer~~ processor of the communication terminal to process at least a portion of the readable medium such that ~~processor,~~ ~~that when read by a processor will~~

~~cause;~~ at least one portion ~~piece~~ of status information is ~~to be~~ stored ~~stored, for a communication terminal,~~ in a memory unit associated with the communication terminal; wherein said at least one portion of status information is ~~to be~~ ~~provided with~~ comprised of a digital signature that is calculated from the status information ~~by means of~~ by a first control unit associated with the communication terminal and is asymmetrically encoded using a private key of the first control unit, the first control unit being ~~for an asymmetrical encoding method associated with a first control unit~~ associated with the communication terminal for the resolution and/or conversion of network addresses; and ~~addresses, wherein said private key is stored remote from the communication terminal;~~

wherein the communication terminal is also configured to determine if the first control unit has failed to properly update the at least one portion of status information and, if the first control unit fails, send ~~to~~ a request to be transmitted to at least one second control unit to associate the communication terminal with the at least one second control unit, the request ~~transmitted~~ comprising ~~the status information and~~ the digital signature, ~~signature~~ ~~to associate the communication terminal with at least one second control unit and a~~ the request configured to initiate a check of the digital signature by the at least one second control unit; and ~~is initiated;~~ in the event of a positive check result, the communication terminal is configured to form an ~~the~~ association ~~of the communication terminal~~ with the at least one second control unit for the resolution and/or conversion of network addresses. ~~unit to be initiated,~~

~~if the control program is running on the computing facility.~~

27. (New) The communication terminal of claim 26 wherein the communication terminal is configured as a PC based communication terminal.

28. (New) The method according to claim 7 wherein the transmission of the request to associate the communication terminal with the at least one second control unit is at least partially defined by a list identifying a plurality of second control units, the list being accessible to the communication terminal.

29. (New) The method of claim 28 wherein the list is stored in the memory of the communication terminal.

30. (New) A method for operating a communication terminal for packet-oriented data transmission, the method comprising:

providing status information for a communication terminal, the status information comprising a digital signature calculated from status information of the communication terminal by a private key of the first control unit such that the digital signature is asymmetrically encoded, the first control unit being associated with the communication terminal for the resolution and/or conversation of network addresses;

storing the status information in a memory unit associated with the communication terminal;

transmitting a request to associate the communication terminal with at least one second control unit if the first control unit is determined to have failed to properly update the status information of the communication terminal, the request comprising the status information and the digital signature;

checking the digital signature with the at least one second control unit; and

associating the communication terminal with the at least one second control unit if the checking of the digital signature results in a positive check result.

31. (New) The method of claim 30 further comprising depositing the public key of the first control unit such that the at least one second control unit is able to access the public key and wherein the at least one second control unit is configured to access the public key of the first control unit to check the digital signature.